International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

OFFTECH TOOL AND END URL FINDER

Sivaprakash S[1], Sasitharan S[2], Shrisanjaykumaar[3], Suresh Kumar P[4]

[1,2,3] Dept. of Electronics and Communication Engineering, Hindusthan College of Engineering And Technology, Coimbatore ,641 032, Tamil Nadu , India
[4]Professor, Dept. Of Electronics and Communication Engineering, Hindusthan College of Engineering And Technology, Coimbatore, 641 032 Tamil Nadu, India

---

Abstract - *Any online web application that is not properly protected is vulnerable to internet attacks these days. Hackers from all around the world can attack your website and steal sensitive data or cause significant damage. Other assaults occur when a user visits a website, for example. The link contains malicious JavaScript code, which can be used to steal personal information or a browser session, as well as lead to a variety of scams. Cybercriminals frequently add links to sensitive websites; however, examining every page on the website for linkages to identity theft is useless, time-consuming, and requires security expertise. Everyone understands the importance of caution, yet it's all too easy to make a mistake by forging an official email. If the link takes you to a bogus website, it may be able to gather detailed information about your device. To avoid this, we must first determine where a link leads before clicking on it. What happens when we click on the link and use a programmer named Offtech Tool and End URL Finder to transfer our personal information.*

Key Words: Offtech tool, End url finder, To find the end face of the fake url, Detect the link or Url, Find the original end face of the fake website link direction, detect the direction the link.

1. INTRODUCTION

Everyone understands the importance of caution, yet it's all too easy to make a mistake by forging an official email. If the link takes you to a bogus website, it may be able to gather detailed information about your device. To avoid this, we must first determine where a link leads before clicking on it. What happens when we click on the link and use a programmer named Offtech Tool and End URL Finder to transfer our personal information. For the scope of this study, mitigation against common attacks on web applications is set, and the webmaster is provided with ways to find criminal hierarchy links to communications developers, research shows the production of web application logs that simplify the process. Analyzing the actions of external users. obsolete, or illegal. Reduction strategies used with secure coding techniques and criminal detection links for sensitive information are developed into a variety of strategies. The advanced application has been tested and tested against various link-based attacks, the results obtained from the test programmer have shown that the website has successfully reduced these malicious web applications attacks, and finding part of the criminal links into critical information, and the best model result provided 98.5% accuracy.

2. EXISTING SYSTEM

Web applications Attack is very popular because many organisations are deploying their resources online. From the attackers' perspective, web applications become vulnerable victims, which is why cyber attacks are one of the biggest threats in the online security sector. These attacks can lead to disruptive effects such as the theft of sensitive information and the removal or editing of the site.

For the scope of this study, mitigation against common attacks on web applications is set, and the webmaster is provided with mechanisms to detect criminal hacking links that target social media developers, the study also shows the production of web application logs that simplify the process of analysing foreign users' actions. , is off-limits, or illegal. Secure coding approaches are used to build mitigation strategies, and different machine learning algorithms and in-depth learning methods are used to develop methods of acquiring a criminal link to steal sensitive information. The advanced application has been tested and tested against a variety of attack scenarios, and the results obtained during the testing process have shown that the website has successfully reduced this attack on malicious web applications, and that comparisons between different algorithms get the best results in detecting part of the criminal links to steal sensitive information.

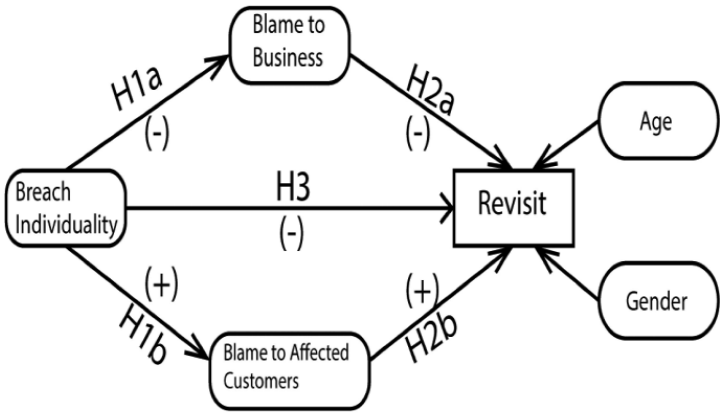

Fig -1: Individual relationships, attitudes, and re-visits are all part of the conceptual paradigm.

Apart from these attacks, identity theft is one of the most common social media attacks, with hackers posing as trustworthy businesses to obtain sensitive and personal information, compromising millions of user records. Log files are used to store website logs in order to track all users' login attempts since they keep track of events and activities. The following is how the paper is organised: The section addresses the problem's definition, the most prevalent Web System Attack, and your mitigating options. displays access records, and the use of machine learning and in-depth reading in the finding of ties to the theft of sensitive information is discussed.

3. PROPOSED SYSTEM

Web Hackers from all around the world can attack your website and steal sensitive data or cause significant harm. Other assaults occur when a person visits a website, for example. The link contains malicious JavaScript code, which may be used to steal personal information or a browser session, as well as lead to a variety of frauds. Cybercriminals frequently add connections to sensitive websites; however, examining every page on the website for linkages to identity theft is useless, time-consuming, and needs security expertise.

Everyone understands the importance of caution, yet it's all too simple to make a mistake by forging an official email. If the link takes you to a bogus website, it may be able to gather detailed information about your device. To avoid this, we must first determine where a link leads before clicking on it. What happens when we click on the link, where we transfer our personal information using a tool called Offtech Tool and End URL Finder.

This programme is independent since it was built for Linux, Windows, Mac, and alover terminal or command promt throughout the arena, and it was also designed for Android.

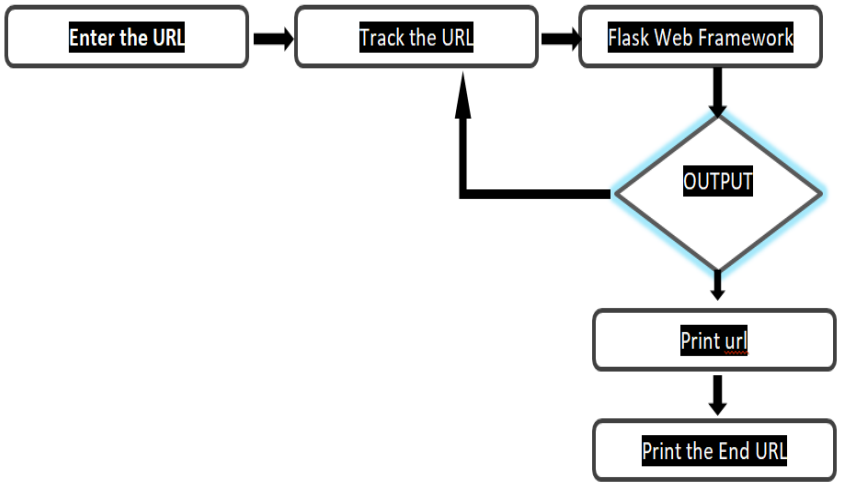

Fig -2: Block Diagram for offtech tool designed by flask framework

3. SOFTWARE USED

Python

PyCharm: This application is self-contained since it was created for Linux, Windows, Mac, and any terminal or command prompt throughout the arena, as well as Android.

Flask Framwork:

Flask is a lightweight Python web framework.

Because they don't require any extra tools or libraries, they're categorised as microframeworks.

It lacks a foundation for webpage summaries, form verification, or any other component where current third- party libraries provide equivalent functionality.

Flask is a Python web application framework that is used in Werkzeug and Jinja2. The following are some of the benefits of utilising the Flask framework: A built-in upgrading server is included, as well as a rapid debugger.

Termux:

Termux is a tool for organising apps downloaded from the Google Play Store (or anywhere else). Activating applications refers to the process of converting bespoke apps into system apps. This can assist prevent programmes from shutting in the background and prevent data loss.

Web Browser:

A web browser is used for offtech output views designed with a flask framework. Output in HTML and CSS.

EX:- chrome, firefox, Microsoft edge or any other web browser.

4. WORKING PROCESS

The Python Flask Web Framework was used to create this web application. Have you ever wondered what happens when this connection is broken? The URL route is followed by Offtech Tool & End Url Finder. Allows you to examine the redirect URL's precise route. It will display a whole URL, shortened link, or sub-URL route redirect.

Fig -3: OffTech tool using Flask framework (in HTML)

Disclosure of Features The following are the essential qualities that have been proved to be successful in detecting identity theft websites: Phishing is classed as a phishing scam if the domain name URL has an IP address.

URL Length - Long URLs may contain malicious content. If the length of the URL is greater than the average length of the URL, then it is classified as suspicious or criminal theft of sensitive information.

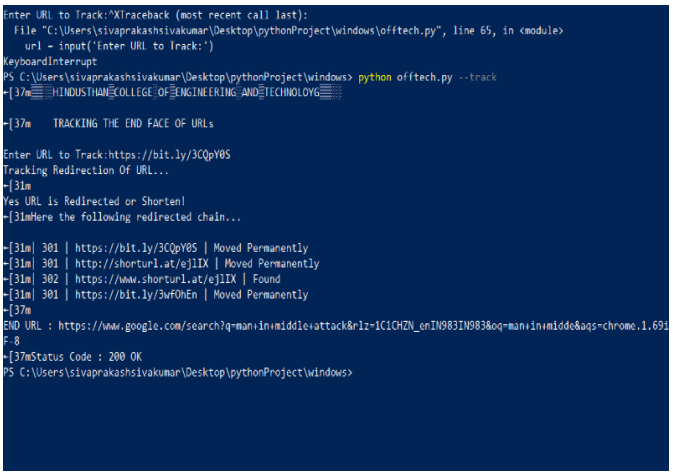

Fig -4: OffTech in Terminal

It is a Python-based Web application. Have you ever wondered where a link leads. The URL route is being followed by Offtech Tool & End url Finder. Allows you to examine the redirect URL's precise route. It will provide a comprehensive list of URLs, shortened links, and sub-URLs that have been redirected.

4. CONCLUSION

The proposed technique with results has shown that the protection scheme works properly with accuracy, sensitivity of this scheme very high for the abnormal and faulty conditions in the link. OFFTECH TOOL will help to identify or recognize the end or original face the link or the URL. If the link have any unwanted redirection between the original link face to the server means it have some unwanted process may it's the way to theft your information or your data. so it's the tool that helps to find the original direction of link and it shows the end face of that URL or a link which has been you submitted. It helps lot of way in this modern network world.

REFERENCES

[1] JAEIL LEE1, YONGJOON LEE2, DONGHWAN LEE3, HYUKJIN KWON4, AND DONGKYOO SHINK "Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups". Received March 30, 2021, accepted May 25, 2021, date of publication May 31, 2021, date of current version June 10, 2021.

[2] Ji-Young, L. J. In, and K. K. Gon, ``The all-purpose sword: North Korea's cyber operations and strategies,'' in Proc. 11th Int. Conf. Cyber Conict (CyCon), Tallinn, Estonia, May 2019, pp. 120.

[3] V. Suganya, ``A review on phishing attacks and various anti phishing techniques,'' Int. J. Computer. Appl., vol. 139, no. 1, pp. 2023,Apr. 2016.

[4] Cybersecurity & Infrastructure Security Agency. North Korean Advanced Persistent Threat Focus: Kimsuky. Accessed: Mar. 31, 2021. [Online].Available: https://us-cert.cisa.gov/ncas/alerts/aa20-301a

[5] K. L. Chiew, K. S. C. Yong, and C. L. Tan, ``A survey of phishing attacks: Their types, vectors and technical approaches,'' Expert Syst. Appl.,vol. 106, pp. 120, Sep. 2018.